

Styrdokument
Dokumenttyp: Regler
Beslutat av: Kommunstyrelsen
Fastställsedatum inkl. dnr: 2026-01-14, §9. Dnr KS.2025.202
Gäller för: Gislaveds kommuns organisation
Ansvarig: Avdelningschef verksamhetsstyrning och it
Revideras: vid behov eller vart fjärde år
Följs upp: It-enheten

Regler för hantering av datorer och mobila enheter

2025-11-26

Innehållsförteckning

1	Syfte	3
2	Omfattning	3
3	Ansvar	3
4	Grundregler för datorer och mobila enheter	3
5	Datorer	4
5.1	Installation och program	4
5.2	Lagring och information	4
5.3	Säkerhetsfunktioner	4
6	Mobila enheter	4
6.1	Användning	4
6.2	Säkerhet	4
6.3	Förvaring och hantering	4
7	USB och tillbehör	5
8	Utlandsanvändning	5
9	Distansarbete	5
10	Förlust, stöld och incidenter	5
11	Återlämning	5

I Syfte

Reglerna säkerställer att kommunens datorer och mobila enheter används på ett sätt som skyddar information, driftmiljö och verksamhetens säkerhet.

2 Omfattning

Reglerna gäller för:

- datorer, mobila enheter, surfplattor och tillbehör
- alla datorer, mobila enheter och surfplattor som ägs, hyrs eller tillhandahålls av kommunen
- medarbetare, förtroendevalda, elever, konsulter och andra som använder kommunens digitala utrustning

3 Ansvar

- Användare ansvarar för att hantera utrustning enligt dessa regler och kommunens säkerhetskrav.
- Chefer ansvarar för att medarbetare, förtroendevalda, elever, konsulter och andra som använder kommunens digitala utrustning känner till och följer reglerna.
- It-enheten ansvarar för konfiguration, säkerhetsinställningar, uppdateringar och tekniska skydd av enheter som tillhandahålls av it-enheten. Informationssäkerhetsfunktionen stödjer med bedömningar och rådgivning.

Brott mot reglerna kan leda till indragen åtkomst, isolering av utrustning, incidentutredning eller arbetsrättsliga åtgärder.

4 Grundregler för datorer och mobila enheter

- Datorer och mobila enheter är arbetsredskap. Privat användning får endast ske i mycket begränsad omfattning och får inte innebära installation av program, lagring av privat material eller åtkomst till privata tjänster utanför webbläsaren.
- Enheter får inte modifieras, låsas upp, inaktivera eller försvaga säkerhetsfunktioner eller användas med icke godkänd programvara.
- Endast av it-enheten godkända och tillhandahållna program, appar, tillägg och säkerhetsinställningar får användas.
- Arbetsinformation ska lagras i kommunens godkända lagringsytor. Lokal lagring på enheten används endast tillfälligt.
- Aktivitet på enheter kan loggas enligt kommunens rutiner.

- Utrustning får inte lämnas obebakad i miljöer där obehöriga kan få åtkomst.
- Säkerhetsmeddelanden och instruktioner från it-enheten ska följas.

5 Datorer

5.1 Installation och program

- Datorer konfigureras av it-enheten.
- Program och tillägg får endast installeras om de är godkända.

5.2 Lagring och information

- Arbetsinformation ska lagras i kommunens godkända lagringsytor.
- Lokal lagring på datorn ska hållas minimal.

5.3 Säkerhetsfunktioner

- Datorer ska vara lösenordsskyddade och låsas när de lämnas obebakade.
- Kryptering och andra säkerhetsfunktioner får inte inaktiveras eller kringgås.

6 Mobila enheter

6.1 Användning

- Arbetsinformation får inte lagras i appar eller tjänster som inte är godkända av kommunen.

6.2 Säkerhet

- Enheter ska skyddas med PIN, lösenord eller biometrisk inloggning.
- Automatisk låsning ska vara aktiverad.

6.3 Förvaring och hantering

- Mobila enheter får inte lämnas synliga i fordon eller allmänna utrymmen.
- Skärmar ska skyddas från insyn vid arbete utanför kontoret.

7 USB och tillbehör

- USB-minnen, lagringsenheter och annan kringutrustning får endast användas om de är godkända och tillhandahålls av it-enheten.
- Privat kringutrustning får inte anslutas.

8 Utlandsanvändning

- Utrustning får tas med utomlands endast om det är godkänt av förvaltningschef och it-enheten i enlighet med rutin.
- Arbetsinformation ska hanteras med särskild försiktighet vid resor.
- It-enheten kan besluta att särskilda säkerhetsåtgärder krävs eller att utrustning inte får tas med.

9 Distansarbete

Distansarbete ska ske enligt regler för it-användning och regler för anslutning till kommunens nätverk.

10 Förlust, stöld och incidenter

- Förlust, misstänkt stöld eller felaktig hantering ska omedelbart rapporteras enligt kommunens incidentrutin.
- It-enheten kan isolera eller spärra utrustning vid misstanke om risk.

11 Återlämning

- Utrustning ska återlämnas när anställning eller uppdrag avslutas, eller när enheten byts ut.
- Enheter ska återställas och raderas enligt kommunens rutiner.
- Privat material eller lokalt sparad information på enheten kan inte återskapas efter återställning.